ELEMENTARY RESULTS ON THE BINARY QUADRATIC FORM $a^2 + ab + b^2$

UMESH P. NAIR

Abstract. This paper examines with elementary proofs some interesting properties of numbers in the binary quadratic form $a^2 + ab + b^2$, where a and b are non-negative integers. Key findings of this paper are (i) a prime number p can be represented as $a^2 + ab + b^2$ if and only if p is of the form $6k + 1$, with the only exception of 3, (ii) any positive integer can be represented as $a^2 + ab + b^2$ if and only if its all prime factors that are not in the same form have even exponents in the standard factorization, and (iii) all the factors of an integer in the form $a^2 + ab + b^2$, where a and b are positive and relatively prime to each other, are also of the same form. A general formula for the number of distinct representations of any positive integer in this form is conjectured. A comparison of the results with the properties of some other binary quadratic forms is given.

1. Background

For more than three centuries, binary quadratic forms and their prime representations have been studied quite extensively. Lagrange was the first to give a complete treatment of the topic, and various mathematicians, including Legendre, Euler and Gauss, contributed to the theory [4, 6].

In addition to the general theory of binary quadratic forms, attempts were made to study the properties of individual forms. The form $a^2 \pm kb^2$ got particular attention, and the prime representations of many such forms have been determined. A list of such representations can be found in [2, p. 71] and [9]. A detailed account of primes of these forms is given in [3].

This paper investigates numbers of the form $a^2 + ab + b^2$, where a and b are non-negative integers, using elementary number theory.

2. Notations and Definitions

The following symbols are used in this paper.

$\mathbb{Z}$	:	Set of integers : $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}^+$	:	Set of positive integers : $\{1, 2, \dots\}$
$\mathbb{Z}^*$	:	Set of non-negative integers : $\{0, 1, 2, \dots\}$
$\mathbb{Q}$	:	Set of rational numbers
$\mathbb{Q}^*$	:	Set of non-negative rational numbers
$\mathbb{R}$	:	Set of real numbers

For convenience, the following definitions are used:

2000 *Mathematics Subject Classification.* Primary 11A67, Secondary 11E16.
Key words and phrases. Binary Quadratic forms, Prime Representation, $a^2 + ab + b^2$.

(1) A $\mathcal{B}$-*representation* is the form a^2+ab+b^2, where $a, b \in \mathbb{Z}^*$ and $a \geq b$.
(2) Two $\mathcal{B}$-representations a^2+ab+b^2 and c^2+cd+d^2 are *distinct* if either $a \neq c$ or $b \neq d$.
(3) An integer is a $\mathcal{B}$-*number* if it has at least one $\mathcal{B}$-representation.
(4) If a $\mathcal{B}$-number is a prime, it is a $\mathcal{B}$-*prime*.
(5) A positive integer is said to be *square-free* if it does not have a square factor greater than 1. In other words, all of its prime factors occur only once in the factorization.

3. General results

3.1. **Some trivial results.** The following are quite obvious from the definition, or can be easily deduced.

Theorem 1. *A number in the form $a^2 \pm ab + b^2$, with $a, b \in \mathbb{R}$, is never negative.*

Proof. WLOG, assume $|a| \geq |b|$. This means $a^2 \geq |ab|$. Since both $a^2 - |ab|$ and b^2 are always non-negative, so is their sum. This proves that both a^2+ab+b^2 and a^2-ab+b^2 are non-negative. □

Theorem 2. *Given $p = a^2+ab+b^2$, where $a, b \in \mathbb{Z}^*$, and the values of p and a, there is a unique b.*

Proof. Given a and p, the value of b is given by

$$b = \frac{-a \pm \sqrt{4p-3a^2}}{2}$$

Since b is nonnegative, only the value corresponding to the positive sign applies here. □

Theorem 3. *If an integer n is in the form a^2+ab+b^2, where $a, b \in \mathbb{Z}$, then n is a $\mathcal{B}$-number, i.e., $n = c^2+cd+d^2$ for some $c, d \in \mathbb{Z}^*$.*

Proof. There are three cases to consider:

(1) *If both a and b are non-negative:* In this case, n is a $\mathcal{B}$-number by definition.
(2) *If both a and b are negative:* Set $c = -a, d = -b$, and now $n = c^2+cd+d^2$, where $c, d \in \mathbb{Z}^*$.
(3) *If one of a and b is negative and other non-negative:* WLOG, assume that $a \geq 0$ and $b < 0$. If $a > -b$, set $c = a+b, d = -b$; else set $c = -(a+b), d = a$. Now, $n = c^2+cd+d^2$, where $c, d \in \mathbb{Z}^*$.

Hence the result. □

It is to be noted that, by Theorem 3, a and b in the $\mathcal{B}$-representation can be any number in $\mathbb{Z}$ in order to get a $\mathcal{B}$-number, but we are restricting the definition to $\mathbb{Z}^*$ only.

3.2. **Identities.** The following identities can be verified easily.

$$c^2(a^2+ab+b^2) - a^2(c^2+cd+d^2) = (bc+ad+ac)(bc-ad) \tag{1a}$$

$$c^2(a^2+ab+b^2) - b^2(c^2+cd+d^2) = (ac+bd+bc)(ac-bd) \tag{1b}$$

$$d^2(a^2+ab+b^2) - a^2(c^2+cd+d^2) = (bd+ac+ad)(bd-ac) \tag{1c}$$

$$d^2(a^2+ab+b^2) - b^2(c^2+cd+d^2) = (ad+bc+bd)(ad-bc) \tag{1d}$$

Theorem 4. *Let $m = a^2 + ab + b^2$, $n = c^2 + cd + d^2$ and $k = mn$, with $a, b \in \mathbb{Z}^*$.*

(1) *$k = \alpha^2 + \alpha\beta + \beta^2$, with $\alpha, \beta \in \mathbb{Z}^*$, has the following solutions:*

$$\begin{cases} \alpha = (ad + bc + bd), & \beta = (ac - bd), & \text{if } ac > bd; \\ \alpha = (ac + ad + bc), & \beta = (bd - ac), & \text{otherwise.} \end{cases} \tag{2a}$$

$$\begin{cases} \alpha = (ac + bd + bc), & \beta = (ad - bc), & \text{if } ad > bc; \\ \alpha = (ad + ac + bd), & \beta = (bc - ad), & \text{otherwise.} \end{cases} \tag{2b}$$

(2) *$k = \alpha^2 + \alpha\beta + \beta^2$, with $\alpha, \beta \in \mathbb{Z}^*$, has the following solutions:*

$$\begin{cases} \alpha = (ad + bc + bd), & \beta = (bd - ac), & \text{if } ac < bd; \\ \alpha = (ac + ad + bc), & \beta = (ac - bd), & \text{otherwise.} \end{cases} \tag{3a}$$

$$\begin{cases} \alpha = (ac + bd + bc), & \beta = (bc - ad), & \text{if } ad < bc; \\ \alpha = (ad + ac + bd), & \beta = (ad - bc), & \text{otherwise.} \end{cases} \tag{3b}$$

$$\alpha = (ad + bc + bd), \quad \beta = (ad + bc + ac). \tag{3c}$$

$$\alpha = (ac + bd + bc), \quad \beta = (ac + bd + ad). \tag{3d}$$

Note that identities (3a–3b) are equivalent to having solutions to $k = \alpha^2 + \alpha\beta + \beta^2$ with non-negative α and non-positive β (by using $-\beta$ instead of β), and identities (3c–3d) is equivalent to having solutions to $k = \alpha^2 + \alpha\beta + \beta^2$ with non-positive α and β (by using $-\alpha$ and $-\beta$ instead of α and β).

3.3. **Known theorems.** The following well-known theorems are used to prove the results in this paper.

Theorem 5 (Fermat)**.** *If p is a prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

This is known as *Fermat's little theorem.* See [7, §6.1].

Theorem 6 (Lagrange)**.** *Let p be a prime and let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, where $p \nmid a^n$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n distinct solutions α such that $-p/2 < \alpha \leq p/2$.*

For a proof, see [1], Theorem 4.4.1.

Theorem 7 (Legendre)**.** *If p is a prime and if k divides $(p-1)$, then the congruence $x^k - 1 \equiv 0 \pmod{p}$ has exactly k distinct solutions between $-p/2$ and $p/2$.*

For a proof, see [1], Corollary 4.4.6.

4. Fundamental form of $\mathcal{B}$-primes

Helguero [6], Fontene [6] and Ramanujan [8, pp. 259–260] observed that every prime other than 3 that can be represented as $a^2 + ab + b^2$ is in the form $6k + 1$. In this section, we prove that it is both the necessary and sufficient condition, and its $\mathcal{B}$-representation is unique (Theorem 8).

Theorem 8. *A prime other than 3 can be represented as $a^2 + ab + b^2$ if and only if it is in the form $6k + 1$, and the representation is unique.*

Theorem 8 states that

(i) a $\mathcal{B}$-prime has a unique $\mathcal{B}$-representation,
(ii) all $\mathcal{B}$-primes other than 3 are in the form $6k + 1$, and

(iii) all primes in the form $6k+1$ are $\mathcal{B}$-primes.

(i) is proved in Theorem 9 by assuming that a $\mathcal{B}$-prime has two $\mathcal{B}$-representations and deducing that they are not distinct.

Theorem 9. *A $\mathcal{B}$-prime has a unique $\mathcal{B}$-representation.*

Proof. Let

$$p = a^2 + ab + b^2 = c^2 + cd + d^2, \tag{4}$$

with $a, b, c, d \in \mathbb{Z}^+$, be two distinct $\mathcal{B}$-representations of the prime p. WLOG, assume $a > c$, so that $ac > bd$. Now, using identities (1d) and (1b),

$$p(d^2 - b^2) = (ad - bc)(ad + bc + bd), \tag{5a}$$

and

$$p(c^2 - b^2) = (ac - bd)(ac + bd + bc). \tag{5b}$$

From (5a), since p is a prime, it should divide at least one of $(ad + bc + bd)$ and $(ad - bc)$. Let us consider each case.

If $p|(ad + bc + bd)$: Since $ac > bd$, using (2a), $p^2 = (ad + bc + bd)^2 + (ad + bc + bd)(ac - bd) + (ac - bd)^2$. Since $ad + bc + bd > 0$, we get $p = ad + bc + bd$, giving $ac = bd$. Now, from (5b), $c^2 - b^2 = 0$, meaning $c = b$, and so, by Theorem 2, $a = d$, showing a unique $\mathcal{B}$-representation of p.

If $p|(ad - bc)$: Here, we have two cases to consider:

If $ad > bc$: By (2b), $p^2 = (ac + bd + bc)^2 + (ac + bd + bc)(ad - bc) + (ad - bc)^2$, and p should divide $(ac + bd + bc)$ as well because p is a prime. Since $(ac+bd+bc) > 0$, this implies $p = (ac+bd+bc)$, meaning $ad = bc$.

If $ad \leq bc$: In a similar way, using (2b), we can show $p = (ad+ac+bd)$ and hence $ad = bc$.

We showed that $ad = bc$ in both cases. Now, from (5a), $d^2-b^2 = 0$, meaning $d = b$, and so, by Theorem 2, $a = c$, showing a unique $\mathcal{B}$-representation of p.

We proved that p has a unique $\mathcal{B}$-representation in both cases. □

(ii) is easily deducible from the properties of congruences (Theorem 10).

Theorem 10. *All $\mathcal{B}$-primes other than* 3 *are of the form* $6k+1$.

Proof. Let $p = a^2 + ab + b^2$ be a prime. Let $a \equiv m \pmod 6$, $b \equiv n \pmod 6$ and $a^2 + ab + b^2 \equiv z \pmod 6$. Now, $m^2 + mn + n^2 \equiv z \pmod 6$, using the basic properties of congruences. For $m = 0 \ldots 5$ and $n = 0 \ldots 5$, z can take only the values $0, 1, 3, 4$, i.e., p can take values $6k$, $6k+1$, $6k+3$ and $6k+4$. Here $6k$ and $6k+4$ are always composite. $6k+3$ is composite except for $k = 0$, i.e., when $p = 3$. So, the only prime values p can take are 3 and $6k+1$. □

(iii) is proved in four steps:

(1) We show that if a $\mathcal{B}$-number is divided by a $\mathcal{B}$-prime, we get another $\mathcal{B}$-number. (Theorem 11)

(2) Using the previous result, we show that if we divide a $\mathcal{B}$-number with a factor that is not a $\mathcal{B}$-number, if such a factor exists, then at least one prime factor of the quotient is not a $\mathcal{B}$-prime. (Theorem 12)

(3) Now we show that every factor of a $\mathcal{B}$-number $a^2 + ab + b^2$, with a and b being relatively prime, is a $\mathcal{B}$-number. We start with the assumption that there is a factor that is not a $\mathcal{B}$-number. We then prove that for any number with that property, we can find a smaller positive number with the same property. Now, by the principle of infinite descent, there is no such number. (Theorem 13)

(4) Finally, using some well-known results, we prove that every prime in the form $6k + 1$ divides a number $a^2 + a + 1$ for some $a \in \mathbb{Z}^+$. Since $a^2 + a + 1$ is a $\mathcal{B}$-number and a and 1 are coprimes, the previous result implies that the prime is a $\mathcal{B}$-prime. (Theorem 15)

Theorem 11. *If a $\mathcal{B}$-number n has a $\mathcal{B}$-prime factor p, then (n/p) is a $\mathcal{B}$-number.*

Proof. Let

$$n = a^2 + ab + b^2, \tag{6}$$

and $n = p \cdot q$, where $p = c^2 + cd + d^2$, with $a, b, c, d \in \mathbb{Z}^*$. We need to prove that q is a $\mathcal{B}$-number.

Consider the identity (1a). Since p divides the LHS, it should divide the RHS. Since p is a prime, it divides at least one of $(bc + ad + ac)$ and $(bc - ad)$. That leads to the following two cases.

Case 1: p divides $(bc + ad + ac)$.

Let $(bc + ad + ac) = rp$, with $r \in \mathbb{Z}$. Set $a = rd + y$ and $b = rc + x$, where $x, y \in \mathbb{Z}$. Combining these, $r(c^2 + cd + d^2) + cx + dy + cy = rp$, which means

$$cx + cy + dy = 0. \tag{7}$$

Now, substituting $a = rd + y$ and $b = rc + x$ in (6) and using (7), we get

$$n = r^2(c^2 + cd + d^2) + x^2 + xy + y^2 + r(cx + dx + dy). \tag{8}$$

Since (7) can be rewritten as

$$c(x + y) + dy = 0,$$

and $(c, d) = 1$, c divides y. Let $y = -cw$, so that $x = (c + d)w$, where $w \in \mathbb{Z}$. Substituting these values of x and y in (8) and simplifying, we get

$$n = (c^2 + cd + d^2)(r^2 + rw + w^2),$$

which means $q = r^2 + rw + w^2$.

Case 2: p divides $(bc - ad)$.

Let $(bc - ad) = rp$, where $r \in \mathbb{Z}$. Set $a = -rd + y$ and $b = rc + x$, where $x, y \in \mathbb{Z}$. Combining these, $rc^2 + cx - dy + rd^2 = rc^2 + rcd + rd^2$, which means

$$rcd + dy - cx = 0. \tag{9}$$

Now, substituting $a = y - rd$ and $b = x + rc$ in (6) and using (9), we get

$$n = r^2(c^2 + cd + d^2) + (x^2 + xy + y^2) + r(cy - dx). \tag{10}$$

Since (9) can be rewritten as

$$c(x - rd) = dy,$$

and $(c, d) = 1$, c divides y. Let $y = cw$, so that $x = (r + w)d$, where $w \in \mathbb{Z}$. Substituting these values of x and y in (10) and simplifying, we get

$$n = (c^2 + cd + d^2)(r^2 + rw + w^2),$$

which means $q = r^2 + rw + w^2$.

So, in either case, $q = r^2 + rw + w^2$, where $r, q \in \mathbb{Z}$. So, by Theorem 3, it is a $\mathcal{B}$-number. □

Theorem 12. *If a $\mathcal{B}$-number n has a factor m which is not a $\mathcal{B}$-number, then (n/m) has at least one prime factor that is not a $\mathcal{B}$-prime.*

Proof. Let $n = m \cdot k$. Factor k into prime factors $k = p_1 \cdot p_2 \cdots p_x$. Suppose that all p_is $(i = 1, 2, \cdots x)$ are $\mathcal{B}$-primes. Now, by Theorem 11, n/p_1 is a $\mathcal{B}$-number, and hence, $n/(p_1 \cdot p_2)$ is a $\mathcal{B}$-number, and continuing this, $n/(p_1 \cdot p_2 \cdots p_x)$ is a $\mathcal{B}$-number, which means m is a $\mathcal{B}$-number, which is a contradiction, so all p_is cannot be $\mathcal{B}$-primes. □

Theorem 13. *If $n = a^2 + ab + b^2$ where $(a, b) = 1$, then each factor of n is a $\mathcal{B}$-number.*

Proof. Suppose that n has a factor p that is not a $\mathcal{B}$-number. Let $a = xp + \alpha$ and $b = yp + \beta$, with $\alpha, \beta \in \mathbb{Z}$, so that $-p/2 < \alpha, \beta \leq p/2$. Since p divides $(a^2 + ab + b^2)$, it should divide $(\alpha^2 + \alpha\beta + \beta^2)$ as well. Let $\alpha^2 + \alpha\beta + \beta^2 = pq$. Since $(\alpha^2 + \alpha\beta + \beta^2) \geq 0$, because of Theorem 1, $pq \geq 0$, and hence $q \geq 0$. Also, since $(\alpha^2 + \alpha\beta + \beta^2) \leq 3p^2/4$, $q \leq 3p/4 < p$.

Let $(\alpha, \beta) = \gamma$. Also let $u = (\alpha/\gamma)$ and $v = (\beta/\gamma)$. Now

$$u^2 + uv + v^2 = \frac{pq}{\gamma^2}.$$

Since γ does not divide p (otherwise γ will divide both a and b), γ^2 should divide q. Let $k = (q/\gamma^2)$. Now,

$$u^2 + uv + v^2 = pk.$$

Since p is not a $\mathcal{B}$-number, because of Theorem 12, k must have a prime factor, say r, that is not a $\mathcal{B}$-prime. Since $r \leq k \leq q < p$, $r < p$.

So, we started with a number $p \geq 0$, which is not a $\mathcal{B}$-number but is a factor of a $\mathcal{B}$-number, and found a smaller number $r \geq 0$ with the same property. So, by the principle of infinite descent, this is impossible. Hence p must be a $\mathcal{B}$-number. □

If $(a, b) = k$, $a^2 + ab + b^2 = k^2x^2 + kx \cdot ky + k^2y^2 = k^2 \cdot (a^2 + ab + b^2)$. So, if a $\mathcal{B}$-number $a^2 + ab + b^2$ is square-free, $(a, b) = 1$. This leads to the following corollary.

Corollary 13.1. *A square-free $\mathcal{B}$-number is the product of $\mathcal{B}$-primes.*

Theorem 14. *For every prime p of the form $6k+1$, there exists a unique positive integer $z < p/2$, such that $z^2 + z + 1 \equiv 0 \pmod{p}$.*

Proof. By Fermat's Little Theorem (Theorem 5),

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \tag{11}$$

Since $(p-1)/2 = 3k$, $x^{p-1} - 1 = (x^{3k} + 1)(x^{3k} - 1)$, and the solutions of (11) are given by the solutions of

$$x^{3k} + 1 \equiv 0 \pmod{p}, \tag{12a}$$

and

$$x^{3k} - 1 \equiv 0 \pmod{p}. \tag{12b}$$

By Theorem 7, (12b) has exactly $3k$ solutions between $-p/2$ and $p/2$. Now, the solutions of (12b) are given by the solutions of

$$x^k - 1 \equiv 0 \pmod{p}, \tag{13a}$$

and

$$x^{2k} + x^k + 1 \equiv 0 \pmod{p}. \tag{13b}$$

(13a) has exactly k solutions such that $-p/2 < x < p/2$, so (13b) should have $2k$ solutions. For any of these $2k$ solutions, $y = x^k$ gives a solution to

$$y^2 + y + 1 \equiv 0 \pmod{p}. \tag{14}$$

Now, any w such that $w = y + k \cdot p$, where $k \in \mathbb{Z}$, also satisfy (14). So, we can find a u such that $-p/2 < u < p/2$ that satisfies $u^2 + u + 1 \equiv 0 \pmod{p}$. Now, setting $v = -(u + 1)$, we find $v^2 + v + 1 = u^2 + u + 1$, so $v^2 + v + 1 \equiv 0 \pmod{p}$. If $u < 0, 0 \leq v < p/2$, and vice versa; so there are at least two solutions, greater than $-p/2$ and less than $p/2$, of which one is negative, and the other is not. But by Lagrange's theorem (Theorem 6), (14) has at most 2 solutions for $-p/2 < y < p/2$. Since p is odd and $p > 1$, we can conclude that (14) has exactly two solutions between $-p/2$ and $p/2$, one a positive integer less than $p/2$, and the other a negative integer greater than $-p/2$. □

Theorem 15. *If a prime number is of the form $6k + 1$, it is a $\mathcal{B}$-prime.*

Proof. Let $p = 6k + 1$ be a prime. By Theorem 14, there exists a $z \in \mathbb{Z}^+$ such that $z^2 + z + 1 \equiv 0 \pmod{p}$. This means $z^2 + z + 1 = m \cdot p$, where $m \in \mathbb{Z}^+$. Since $(z, 1) = 1$, by Theorem 13, every factor of $z^2 + z + 1$ should be a $\mathcal{B}$-number, so p is a $\mathcal{B}$-prime. □

Proof of Theorem 8 follows from Theorems 9, 10 and 15.

5. Factors of $\mathcal{B}$-numbers

In this section, we prove the following theorem.

Theorem 16. *The necessary and sufficient condition of any non-negative integer to be in the form $a^2 + ab + b^2$ is that, in its prime factorization, all primes other than 3 that are not in the form $(6k + 1)$ have even exponents.*

The *sufficient* part is proved first:

Theorem 17. *If the factorization of a number has even exponents for all primes other than 3 and those in the form $(6k + 1)$, the number is a $\mathcal{B}$-number.*

Proof. From (2a), the product of any numbers of $\mathcal{B}$-numbers is a $\mathcal{B}$-number. In particular, the product of any number of $\mathcal{B}$-primes is a $\mathcal{B}$-number. Since every square is a $\mathcal{B}$-number, multiplying a $\mathcal{B}$-number with a square will yield a $\mathcal{B}$-number. Hence, the product of any number of $\mathcal{B}$-primes and any square is a $\mathcal{B}$-number.

The theorem easily follows from this. □

We prove the *necessary* part as follows:

(1) We prove that if we divide a $\mathcal{B}$-number by a square factor, if it has one, the quotient is a $\mathcal{B}$-number.(Theorem 18)
(2) Now, using Corollary 13.1, the result follows.

Theorem 18. *If the product of m and k^2, with $m, k \in \mathbb{Z}^+$, is a $\mathcal{B}$-number, then m is a $\mathcal{B}$-number.*

Proof. We have

$$a^2 + ab + b^2 = k^2 \cdot m. \tag{15}$$

Let s^2 be the largest square factor of m. Let $n = m/s^2$. We need to only show that n is a $\mathcal{B}$-number, because, m, being the product of two $\mathcal{B}$-numbers, is a $\mathcal{B}$-number then. Now, defining $p = ks$, (15) becomes

$$a^2 + ab + b^2 = p^2 \cdot n,$$

where n does not have square factor > 1. Let $g = (a, b)$ and $c = a/g, d = b/g$. Now $g^2(c^2 + cd + d^2) = p^2 n$, or

$$c^2 + cd + d^2 = \frac{p^2}{g^2} \cdot n.$$

Since g^2 doesn't divide n if $g > 1$, p/g must be an integer. Now, by Theorem 13, each factor of the LHS must be a $\mathcal{B}$-number, so each factor of n must be a $\mathcal{B}$-number. So, n, being the product of $\mathcal{B}$-numbers, must be a $\mathcal{B}$-number. □

Theorem 19. *Every prime factor, which is not a $\mathcal{B}$-prime, of a $\mathcal{B}$-number has even exponents in the standard form of expansion.*

Proof. Let n be any $\mathcal{B}$-number and let s^2 be its largest square factor. By Theorem 18, (n/s^2) is a square-free $\mathcal{B}$-number, which is, by Corollary 13.1, the product of $\mathcal{B}$-primes. So, all non-$\mathcal{B}$-prime factors should be contained in s^2, hence should have even exponents. □

Proof of Theorem 16 follows from Theorems 17 and 19.

6. General form of a $\mathcal{B}$-number

From the already proved theorems, the general form of a $\mathcal{B}$-number is

$$n = x^2 \cdot 3^y \cdot a^\alpha \cdot b^\beta \cdot c^\gamma \dots \tag{16}$$

where

x	:	Some number in $\mathbb{Z}^*$, with no prime factor in the form $6k+1, k \in \mathbb{Z}^+$.
y	:	Some number in $\mathbb{Z}^*$
$a, b, c, \dots$	:	A prime in the form $6k + 1, k \in \mathbb{Z}^*$
$\alpha, \beta, \gamma, \dots$	:	Some number in $\mathbb{Z}^*$

A number is a $\mathcal{B}$-number if and only if it can be represented in the form (16).

Conjecture 1. *The number of distinct $\mathcal{B}$-representations of a $\mathcal{B}$-number represented in the form given by* (16)*, counting the cases when $a = b$ and when either of a or b is zero, is given by*

$$\begin{cases} \frac{1}{2}\Big(1 + (\alpha+1)(\beta+1)(\gamma+1)\dots\Big), & \text{if all of } \alpha, \beta, \gamma, \dots \text{ are even;} \\ \frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)\dots, & \text{otherwise.} \end{cases} \tag{17}$$

The reader will recognize that (17) is the same as the expression for the number of distinct representations of a number as a sum of two squares, a result given by Gauss and Legendre, later proved by Jacobi and others [5]. This expression applies here also, with a different definition of the individual parameters. A proof is not attempted in this paper.

7. $\mathcal{B}$-numbers in terms of rational numbers

Theorem 20 extends the domain of a and b in the previous theorems from $\mathbb{Z}^*$ to $\mathbb{Q}^*$.

Theorem 20. *If a number n is representable as $\alpha^2 + \alpha\beta + \beta^2$, where α and β are positive rational numbers, then n is a $\mathcal{B}$-number.*

Proof. Let $\alpha = (a/b)$ and $\beta = (c/d)$. Now

$$\begin{aligned} n &= \alpha^2 + \alpha\beta + \beta^2 \\ &= \left(\frac{a}{b}\right)^2 + \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) + \left(\frac{c}{d}\right)^2 \\ &= \frac{a^2d^2 + abcd + b^2c^2}{b^2d^2} \end{aligned}$$

Hence,

$$n \cdot (bd)^2 = (ad)^2 + (ad)(bc) + (bc)^2$$

Then, by Theorem 18, n is a $\mathcal{B}$-number. □

8. Comparison with the form $a^2 - ab + b^2$

Being another binary quadratic form with the same discriminant, the form $a^2 - ab + b^2$ shares many properties with $a^2 + ab + b^2$.

All primes in the form $6k + 1$ and 3 can be represented as $a^2 - ab + b^2$, but this representation is not unique. In general, if $n = a^2 + ab + b^2$, where $n \in \mathbb{Z}^*$, then n can be represented as $x^2 - xy + y^2$ in two ways by setting $x = a, y = a + b$ and $x = b, y = a + b$. The unique representation occurs only when $a = b$, i.e., when $n = 3a^2$, and 3 is the only prime that has unique representation. Similarly, when $n = a^2 - ab + b^2$, with $a \geq b$, n can be represented as $x^2 + xy + y^2$ as well, by setting $x = a - b, y = b$. Because of this equivalence, all results in this paper, except Theorem 8, Theorem 9 and (17), are valid for the form $a^2 - ab + b^2$ as well.

9. Comparison with forms equivalent to $ka^2 + kab + kb^2$

Many results discussed in this paper have been proved for some of the binary quadratic forms equivalent to $ka^2 + kab + kb^2, k \in \mathbb{Z}^+$. For example, Euler (1763) proved the following for the form $a^2 + 3b^2$ [6], which is equivalent to $2a^2 + 2ab + 2b^2$.

(1) A prime p can be represented in this form if and only if $p = 3$ or $p \equiv 1 \pmod 6$ (cf. Theorem 8). Goring (1874) proved the uniqueness of this representation (cf. Theorem 9).
(2) Every prime divisor (other than 2) of a number in this form, with a and b coprimes, is itself in this form (cf. Theorem 13).

Similar analogies can be found for forms equivalent to any $ka^2 + kab + kb^2$, like $a^2 + ab + 7b^2$, $a^2 + 12b^2$, $3a^2 + 4b^2$, $a^2 + ab + 19y^2$, $3a^2 + 3ab + 7b^2$, etc.

10. Comparison with the form $a^2 + b^2$

Every theorem in this paper has an analogous theorem for the form corresponding to the sum of two squares. They are listed below:

(1) (L. Pisano, 1225) The product of two numbers can be expressed as the sum of two squares if the individual numbers can be. [5, Ch. 6] (cf. Theorem 4.)

(2) (Euler, 1749) A prime p can be expressed as the sum of two squares if and only if $p \equiv 1 \pmod 4$, with the only exception of 2. (cf. Theorem 8.) Gauss proved that this representation is unique. (cf. Theorem 9)
(3) (Euler, 1749) If $m = a^2 + b^2 = pl$, where $p = c^2 + d^2$ is a prime, then l is the sum of two squares. [1, §7.1] (cf. Theorem 11)
(4) (Euler, 1749) Let $m = a^2 + b^2 = nk$. If k is not a sum of two squares, then n has a prime factor which is not a sum of two squares. [1, §7.1] (cf. Theorem 12.)
(5) (Euler) A positive number is the sum of two squares if and only if all of its factors in the form $4m+3$ have even exponents in the standard factorization. [7, Th. 366] (cf. Theorem 16.)
(6) (Goldbach, 1743) A prime $4k - 1$ cannot divide the sum of two relatively prime squares. [5, Ch. 6] (cf. Theorem 13.)
(7) -1 is a quadratic residue of primes of the form $4k + 1$ [7, Th. 82]. This means there exists a positive integer z such that $z^2 + 1 \equiv 0 \pmod p$ if $p = 4k + 1$ is a prime. (cf. Theorem 14.)
(8) If $n = \alpha^2 + \beta^2$, where α and β are rational, then n is the sum of two integer squares. [1, Note 7.1.5] (cf. Theorem 20.)
(9) (Gauss, 1801) The general form of a number n that can be expressed as the sum of two squares is

$$n = x^2 2^y a^\alpha b^\beta c^\gamma \dots \tag{18}$$

where $a, b, c, \dots$ are primes of the form $4k + 1$, and x is the product of primes of the form $4k + 3$. (cf. (16).)
(10) Jacobi (1834) gave an expression for the number of representations of a number n in the form $a^2 + b^2$, which, when applied to distinct representations with a and b in $\mathbb{Z}^*$, reduces to (17), when n is expressed as in (18). (cf. (16) and (17).)

11. Conclusions

Many mathematicians have observed the properties of the form $a^2 + ab + b^2$ and similar forms, and quite an extensive study of binary quadratic forms has been done in the past. Many of the results in this paper can be obtained using alternate techniques. One such method is to assume the already known properties of the form $a^2 + 3b^2$, and then deduce the result for $a^2 + ab + b^2$ by trivial substitutions.

The contribution of this paper is the proof to these properties by elementary theory of numbers. It also conjectures a formula for the number of representations of a number in the form.

This paper proves that the binary quadratic form $a^2 + ab + b^2$ has properties very much analogous to those of the form $a^2 + b^2$. It is possible that these are two special cases of a more general form. More investigation is needed in this area.

References

[1] R.B.J.T. Allenby and E.J. RedFern, *Introduction to number theory with computing*, Oxford Science Publications, 1995.
[2] B.C. Berndt, *Ramanujan's notebooks, part iv*, Springer-Verlag, 1994.
[3] D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons Inc., 1989.
[4] H. Davenport, *The higher arithmetic, 7th ed.*, Cambridge University Press, 1999.

[5] L.E. Dickson, *History of the theory of numbers, vol. 2, reprint of the 1920 edition*, AMS-Chelsea, 1999.
[6] ———, *History of the theory of numbers, vol. 3, reprint of the 1923 edition*, AMS-Chelsea, 1999.
[7] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers, 5th. ed.*, Oxford Science Publications, 1995.
[8] S. Ramanujan, *Ramanujan's lost notebook and other papers*, Narosa Publishing House, Bombay, 1988.
[9] E.W. Weisstein, *Prime representation*, From MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeRepresentation.html.

Mentor Graphics Corporation, 8005 SW Boeckman Road, Wilsonville, OR 97070, USA.
E-mail address: umesh_nair@mentor.com